Office of the Governor
State Chief Information Officer

SECURITY

Chapter 3 – Processing Information and Documents

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Networks

030101 Configuring Networks

Purpose: To establish a framework for the configuration of networks.

STANDARD

Agency network infrastructures shall be designed and configured using controls to safeguard the State's information systems. Failure to protect network infrastructures against threats can result in the loss of data integrity, data unavailability and/or unauthorized data use. Secure configuration of the network infrastructure shall include but not be limited to the following:

- All hardware connected to the State Network shall be configured to support agency management and monitoring standards.
- The cabled network infrastructure must comply with industry standards and be installed by a licensed, bonded contractor.
- Perimeter defense systems, including routers and firewalls, and network-connected equipment, including switches, wireless access points, personal computers and servers, shall be configured to secure specifications approved by security institutes such as the SANS Institute or the National Security Agency (NSA).
- All network address space (Internet Protocol [IP]/Internet Packet Exchange [IPX]) shall be distributed, registered and managed by ITS.
- Critical hardware and systems, including the network infrastructure, shall be connected to an uninterruptible power supply (UPS).
- Network devices shall be configured to support authentication, authorization and accountability mechanisms when being administered.
- Configuration management, patch management and change management standards and procedures shall be applied to all applicable systems.
- Extending, modifying or retransmitting network services, such as through the installation of new switches or wireless access points, in any way is prohibited, unless prior approval is granted.

- Configuration shall include elimination of the possibility of bridging networks via secondary Internet connections.
- Network servers/services such as email, Web, and ftp shall be segregated from an agency's internal user LAN.
- Configuration shall include accommodations for flexibility, scalability and reliability to meet growing user demands and conserve IT funds of the future.

ISO 17799: 2005 References

10.6 Network security management
11.4 Network access control
11.4.2 User authentication for external connections

030102 Managing the Networks

Purpose: To establish a framework for the management and protection of the State's network resources.

STANDARD

Agencies' network infrastructure shall be managed using controls to safeguard the State's information systems. Failure to protect against threats can result in loss of data integrity, data unavailability and/or unauthorized use of data.

Secure management of the network infrastructure shall include but not be limited to the following:

- Use of secure protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), Internet Protocol Security (IPSec), Simple Network Management Protocol (SNMP) version 3, etc., for network management.
- Use of authentication, authorization and accountability mechanisms when administering network devices.
- Monitoring for attempts to deny service or degrade the performance of information systems (including computers, microcomputers, networks, telephone systems and video systems).
- Restriction of transfers of large amounts of data between computing systems during business hours, unless required or authorized by senior management.
- Definition of tasks/roles/responsibilities involved in management and security of agency IT resources in job descriptions.

ISO 17799: 2005 References

8.1 Prior to employment
10.6.1 Network controls
11.4.1 Policy on use of network services
11.4.2 User authentication for external connections

030103 Accessing Your Network Remotely

Purpose: To require users to access agency information technology systems in a secure manner.

STANDARD

Agencies may permit authorized users of their computer systems, networks and data repositories to remotely connect to necessary systems, networks and data repositories for the purpose of conducting agency-related business only. Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed.

In addition, remote accessing of networks and systems shall include but not be limited to the following:

- Administrators shall take all precautions necessary to ensure that administrative activities performed remotely cannot be intercepted or spoofed by others. Guidance: configure timestamps, encryption, and/or dial-back mechanisms.
- Enhanced authentication and encryption mechanisms shall be used to protect data used for remote management of network devices or servers.
- Systems connecting remotely to agencies connected to the State Network must have antivirus software installed compliant with the statewide antivirus standard.
- Systems connecting remotely to agencies connected to the State Network must have the latest operating system and application patches installed.
- Access to diagnostic ports (especially dial-up diagnostic ports) shall be securely controlled and enabled only when needed for authorized diagnostic access.
- All users wishing to establish a remote connection via the Internet to the agency's internal network must first authenticate themselves at a firewall or security device.
- Inbound and outbound network traffic shall be controlled and limited to only that necessary to accomplish the State's mission, using a perimeter firewall and host-based firewall compliant with the statewide firewall standards.
- Virtual private networks (VPNs) shall require user authentication and encryption strength compliant with the statewide encryption standard.
- Internal addresses, configurations, dial-up modem numbers, and related system design information for the State's networking systems shall be kept secret and not made public knowledge.
- Administrators must gain agency chief information officer (CIO) approval for any modem installed at a workstation and must not leave modems connected to computers that have auto-answer mode enabled.[1]
- All dial-up connections with the State's systems and networks must be routed through a modem pool that includes an approved user authentication system.

ISO 17799: 2005 References

11.4.2 User authentication for external connections.

030104 Defending Network Information from Malicious Attack

Purpose: To protect information residing on State and agency networks.

[1] Unless the modem is needed for business purposes, it is recommended that, in systems with built-in modems that cannot be removed from the machine, the modem driver be uninstalled and the modem device be disabled within the operating system to disable the modem functionality.

STANDARD

Agencies shall implement layers of information security (defense in depth) to defend against attacks on the State's information resources.

All safeguards and network security plans shall incorporate the following controls:

- Configuration of system hardware, operating systems and applications software and network and communication systems to information security standards and secure specifications set by ITS. When such standards do not exist, agencies are expected to conform to industry guidelines and security standards from institutes such as the SANS Institute or the National Security Administration (NSA).
- Implementation of preventive measures to limit internal and external parties' abilities to inflict harm on the State's information technology resources.
- Implementation of measures to prevent snooping, sniffing, network reconnaissance and other means of gathering information about the network infrastructure.
- Implementation of measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network.
- Installation of antivirus software that protects the State's infrastructure from downloads, media transfers electronic-mail attachments of malicious software, or other malware.
- Continuous monitoring for attempts to deny service or degrade the performance of information systems (including computers, microcomputers, networks, telephone systems and video systems).
- Periodic review of system logs for signs of misuse, abuse or attack.

GUIDELINES

Agencies should consider technologies that eliminate single points of failure on critical systems. Examples of such technologies are server clustering, redundant links, link load balancing and redundant array of independent disks (RAID) backups.

ISO 17799: 2005 References
10.4.1 Controls against malicious code

030105 Network Segregation

Purpose: To help protect internal networks through network segregation.

STANDARD

Agencies' internal network infrastructures (i.e., agency local area networks [LANs]) shall be segregated into internal network domains to protect servers from the user LAN and to segregate test and production environments.

Wireless networks shall be physically or logically segregated from internal networks such that an unknown external user cannot access an agency's internal network unless it was designed for that specific use.

GUIDELINES

Agencies should consider segregating network management protocols onto a separate internal network domain from the production domain. For example, network monitoring traffic and network administration traffic should be logically segregated from end users and from the production network.

Segregation may be achieved by one or both of the following common methods or through similar methods of achieving logical segregation:

- Implementing virtual LANs (VLANs) with access control lists in a switched network environment.
- Using routers or internal firewalls with access control lists.

RELATED INFORMATION

Standard 020115 – Access Control Framework
Standard 090301 – Electronic Eavesdropping

ISO 17799: 2005 References
11.4.5 Segregation in networks

030106 Controlling Shared Networks

Purpose: To control access to shared networks.

STANDARD

Shared networks shall be restricted according to the agency's access control policy, application usage requirements, and the user's job responsibilities.

GUIDELINES

Network gateways (firewalls, routers, remote access servers, etc.) can be used to restrict users' connection capabilities through the use of protocol filters, access control lists, and time-based rules[2].

ISO 17799: 2005 References
11.4.6 Network connection control

030107 Routing Controls

Purpose: To protect access to the State's routed networks.

STANDARD

Agencies shall deploy mechanisms to control access to the State's network backbone and/or routed infrastructure. Protective controls shall at a minimum include the following:

[2] Time-based rules can be used to restrict access for certain groups of users to specific time periods. For example, an Agency's users could be granted 24-hour access while limiting all other access to users during business hours only.

- Positive source and destination address checking to restrict rogue networks from manipulating the State's routing tables.
- Authentication to ensure that routing tables do not become corrupted with false entries.
- Network address translation (NAT) to screen internal network addresses from external view.

ISO 17799: 2005 References
11.4.7 Network routing control

030108 Network Security

Purpose: To protect the integrity and ensure the stability of the statewide network from fraudulent use and/or abuse resulting from access and use of the network and to define the security attributes delivered with network services.

STANDARD

ITS is responsible for the security of the infrastructure of the state's network and is bound by the terms and conditions of its upstream network providers as well as enterprise security standards and policies.

Organizations with connections to the state network are responsible for managing risk and providing appropriate security for their networks. Security measures must conform to applicable enterprise network security standards, architecture, and policies. Agency internal security measures shall be deployed only on agency internal networks and must not adversely affect the state network.

Any and all actions that jeopardize the integrity and stability of the state network will be addressed commensurate to the level of risk. ITS is authorized to immediately suspend network service to any organization when the level of risk warrants immediate action. When network service is suspended, ITS will provide immediate notice to the organization. When possible, ITS will notify any organization of any such action in advance of such an action. ITS will work with the organization to rectify the problem that caused the suspension. Any violations of this network security standard are subject to review by the State Chief Information Officer (State CIO) and organization management and are subject to action that conforms to state disciplinary policies and any and all relevant law. These actions may include termination of service. Termination requires appropriate notification by ITS, including notification to its upstream providers, and the termination should be at the lowest level necessary to safeguard network security and minimize disruption of business activities.

Network service agreements shall specify detailed information and requirements regarding the security features, service levels, and management requirements for all network services provided. When network services are outsourced, the agreement shall include provisions for the agency to monitor and audit the outsourced provider's adherence to the agreement.

RELATED INFORMATION

070104 Using External Service Providers for E-Commerce

ISO 17799: 2005 References
10.6.2 Security of network services

030109 Time-out Facility

Purpose: To prevent network misuse, and unauthorized access through the implementation of time-out mechanisms.

STANDARD

Agencies shall implement time-out mechanisms that terminate sessions after a specified period of inactivity, such that the user must re-authenticate his identity to resume the session. If the user is connected via external networks (e.g., a telecommuter logging in from home), the time-out mechanism must also terminate the network connection.

All terminals, workstations, and laptops connected to the agency network shall enable a terminal time-out mechanism to prevent unauthorized viewing or use when the terminal, workstation, or laptop is unattended.

The period of inactivity for session and terminal time-outs shall be established based on the agency's needs; system or application criticality; the confidentiality of the information accessed through the system or application; or other risk factors, but shall not exceed 30 minutes.

GUIDELINES

Terminal time-outs may be achieved through the use of agency approved, password protected screen savers (sometimes called "screen locks").

ISO 17799: 2005 References
11.5.5 Session time-out

030110 Exploitation of Covert Channels

Purpose: To limit the risk of information leakage through the use and exploitation of covert channels.

STANDARD

Agencies shall mitigate risks of exploitation of covert channels by obtaining third-party applications from reputable sources and by protecting the source code in custom developed applications.

See the Related Information section, below, for references to the policies that address specific protection mechanisms.

RELATED INFORMATION

030301 Downloading Files and Information from the Internet

030304 Receiving Electronic Mail

030314 "Out of the Box" Web Browser Issues

030318 Certainty of File Origin

030505 Receiving Information on Disks

030902 Loading Personal Screen Savers

060107 Defending Against Hackers, Stealth- and Techno-Vandalism

060109 Defending Against Virus Attacks

060111 Installing Virus Scanning Software

080201 Software Development

080206 Separating Systems Development and Operations

ISO 17799: 2005 References
12.5.4 Information leakage

030111 Authentication of Network Connecting Equipment

Purpose: To control and/or detect the installation of unknown equipment on a network.

STANDARD

To protect the State Network from vulnerabilities that can be introduced when users access the network with unmanaged devices, agencies shall require that all users accessing the State Network with any devices adhere to required security configurations for those devices, including required patches and updated anti-virus signature files on those devices.

GUIDELINES

Equipment identification may be achieved through various methods, including validation of the media access control (MAC) address, validation of other unique equipment identifiers, or through the use of digitally signed certificates that are associated with a specific server or device.

Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal subnetworks ("subnets").

ISO 17799: 2005 References
11.4.3 Equipment identification in networks

Section 02 System Operation and Administration

030201 Appointing System Administrators

The standard recommended by ISO 17799 in this category is properly addressed by the State Office of Personnel and each agency's personnel office.

ISO 17799: 2005 References
6.1.3 Allocation of Information Security responsibilities

030202 Administering Systems

Purpose: To establish security roles and duties for system administrators.

STANDARD

Agencies must clearly define security responsibilities for system administrators, who shall protect their assigned information technology resources and the information contained on those resources. Agencies must also provide appropriate training for their system administrators.

System administrators shall:

- Ensure that user access rights and privileges are clearly defined, documented and reviewed for appropriateness.
- Consider the risk of exposure when administering system resources.
- Take reasonable actions to ensure the authorized and acceptable use of data, networks and communications transiting the system or network.

ISO 17799: 2005 Reference
6.1.3 Allocation of Information Security responsibilities

030203 Controlling Data Distribution

Purpose: To protect the State's data and information from unauthorized disclosure.

STANDARD

Technical access controls or procedures shall be implemented to ensure that data and information are distributed only as authorized and as appropriate. Access controls and/or procedures shall, in part, be based on agency business requirements. Once a business justification is provided, personnel shall adhere to the following standards:

- If information includes both confidential data and data available for public inspection, the classification level shall default to confidential.
- Electronic media entering or leaving offices, processing areas or storage facilities shall be appropriately controlled.
- Storage areas and facilities for media containing confidential data shall be secured and all filing cabinets provided with locking devices.
- Confidential information shall not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements and return dates.
- When confidential information is shipped, the delivery shall be verified.
- If confidential information is sent via the Internet or other unsecured media transmission facility, the information must be encrypted during transmission.

ISO 17799: 2005 Reference
9.1 Secure Areas

030204 Permitting Third-Party Access

Purpose: To secure third-party access and prevent unauthorized access to information systems and data.

STANDARD

Agencies shall implement security controls in accordance with Standard 020104, Managing Network Access Controls, and Standard 090104, Physical Access Control to Secure Areas, when granting third-party access to agency information systems. Third-party contracts shall specify the access, roles and responsibilities of the third party before access is granted.

ISO 17799: 2005 Reference

6.2.1 Identification of risks from third party access

030205 Managing Electronic Keys

Purpose: To ensure that electronic key systems are managed under proper controls.

STANDARD

When an agency implements an electronic key system, it must establish proper controls to protect the key and the data encrypted. The system must be designed so that no single person has full knowledge of any single key. The system design must also ensure that:

- Separation of duties or dual control procedures are enforced.
- Any theft or loss of electronic keys results in the notification of management.
- All keys are protected against modification and destruction, and secret/private keys are protected against unauthorized disclosure.
- Physical protection is employed to protect equipment used to generate, store and archive keys.
- A dual-control electronic key recovery system is documented and in place. This shall be handled through key escrow procedures.
- Encrypted data are recoverable.

Agencies also must comply with the applicable regulations established by the North Carolina Secretary of State.

ISO 17799: 2005 References

12.3.1 Policy on the use of cryptographic controls
12.3.5 Key management

030206 Managing System Operations and System Administration

Purpose: To ensure that agency systems are operated and administered using documented procedures that are efficient and effective in protecting the agency's data.

STANDARD

Agencies shall employ and document controls to provide for the management of system operations and system administration.

To minimize the risk of corruption to operating systems or integrated applications, the controls shall include, but not necessarily be limited to, the following:

- Assigned staff shall perform the updating of the operating systems and program/application backups.
- Operating system software patches shall be applied only after reasonable testing verifies full functionality.
- Physical or logical access shall be given to suppliers for support purposes only when necessary and with documented management approval. The suppliers' activities shall be continuously monitored.

GUIDELINES

- Whenever possible, critical applications should be separated from databases.
- An audit log should be maintained to reflect all updates to operational program libraries.
- Vendor-supplied software used in operating systems should be maintained at a level supported by the vendor. Any decision to upgrade should take into account the security of the release (i.e., the introduction of new security functionality).

ISO 17799: 2005 References
10.10.4 Administrator and operator logs
12.4.1 Control of operational software

030207 Managing System Documentation

Purpose: To ensure that the system documentation for all the organization's information systems is accurate and available.

STANDARD

Agencies shall control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting and staff turnover. Examples of system documentation include descriptions of applications processes, procedures, data structures and authorization processes.

The following controls must be considered to protect and maintain system documentation:

- Internal system documentation must be stored securely and in an area known by management.
- Access to internal system documentation must be limited and be authorized by management.
- Documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures and/or authorization processes.

ISO 17799: 2005 References
10.7.4 Security of system documentation
12.5.1 Change control procedures

030208 Monitoring Error Logs

Purpose: To protect agency information technology assets from unintentional and malicious attacks.

STANDARD

Error logs generated by information technology systems shall be regularly monitored and reviewed for abnormalities and shall be:

- Cross-checked for known security events based on network, size, system type and logical and physical location.
- Enabled on each device or system on the network, such as servers, firewalls, routers, switches, cache engines, intrusion detection systems (IDSs) and applications, as long as performance requirements are not affected.
- Monitored on a weekly basis at a minimum.
- Routinely checked for time and date accuracy. See Standard 030212, Synchronizing System Clocks, for more on clock synchronization.
- Retained as required under the agency records retention policy or the General Schedule for State Agency Records, Information Technology Records.

Error logs shall be checked against baselines to effectively verify variations from normal work-related activities.

The confidentiality, integrity and availability of error logs shall be safeguarded.

ISO 17799 References

10.10.1 Audit logging
10.10.2 Monitoring system use
10.10.3 Protection of log information

030209 Scheduling System Operations

Purpose: To ensure that modifications to information system operations are implemented and maintained properly.

STANDARD

To maintain the highest level of system availability and protect the agency's infrastructure, maintenance operations must be performed at predetermined, authorized times or on an approved, as-needed basis.

Documented operational procedures must be created, implemented and maintained during system operations and take into consideration:

- Computer start up, shutdown, and recovery procedures.
- Scheduling requirements (length, time frame, etc.).
- Processes for handling errors and unforeseen issues that may arise during job execution.
- Contact lists.

- System restrictions.
- Instructions for handling output, including failed jobs.
- Proper media handling and storage.
- Incident handling and escalation procedures.
- Configuration management.
- Patch management.
- General system hardware and software maintenance.
- All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.
- When special or emergency situations make it necessary to perform maintenance operations outside of the normal system operations schedule, these situations must be documented, management must be notified, and the operation processes used must be recorded.

ISO 17799: 2005 Reference
10.1.1 Documented operating procedures

030210 Scheduling Changes to Routine System Operations

Purpose: To ensure that the State's information system operations change control procedures are adequate and properly implemented and documented.

STANDARD

Agencies shall develop change control procedures to accommodate resources or events that require changes to system operations. Changes to system baselines require effective communication to ensure that information systems maintain secure operations and avoid lag due to processing consumption and to minimize downtime due to unforeseen problems during such changes.

Change control procedures must be documented and followed during the scheduled maintenance windows and take into consideration:

- Periods of maximum and minimum workflow.
- The approval and notification process.
- Interfaces with other applications, systems or processes.
- External agency and departmental interdependencies.
- Change categories, risk and type.
- The change request process.
- Rollback plans and the point of no return.
- Modifications to change control procedures for special or emergency circumstances.

All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy.

Upon the completion of a baseline change, the audit change logs must be retained in accordance with the General Schedule for State Agency Records, Information Technology Records as established by the Government Records Branch of the Department of Cultural Resources.

ISO 17799: 2005 References
10.1.2 Change management

030211 Monitoring Operational Audit Logs

Purpose: To protect the integrity and availability of information systems by monitoring operational audit logs.

STANDARD

Agencies shall designate trained staff to regularly review operational audit logs, including system, application and user event logs, for abnormalities. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to management. Because they also provide an audit trail in the event of a security incident, operational audit logs shall include the following:

- User ID responsible for system restart or shutdown and date and time of restart or shutdown.
- User ID responsible for application start up, restart and/or shutdown and date and time of start up or shutdown.
- Attempts to create, remove or set passwords or change system privileges.
- Successful and failed login attempts.
- Unauthorized attempts to access network and system files.
- Attempts to initialize, remove, enable or disable accounts or services.
- System errors and corrective action(s) taken.
- Failed read-and-write operations on the system directory.

Personnel responsible for audit logs must ensure:

- That the agency has established a current, reliable baseline that can be compared to audit logs to determine whether any abnormalities are present.
- That all operational audit logs are retained in accordance with the General Schedule for State Agency Records, Information Technology Records as established by the Government Records Branch of the Department of Cultural Resources.

ISO 17799: 2005 References
10.10.4 Administrator and operator logs
15.3.1 Information systems audit controls

030212 Synchronizing System Clocks

Purpose: To prevent operations failure, data loss or security holes resulting from the inaccuracy of system clocks.

STANDARD

To maintain the correct time and accuracy of audit logs on information systems residing within the State Network, system clocks must be synchronized regularly across various agency platforms.

System time clocks must be updated on a daily basis from a time source that agrees with the Coordinated Universal Time, and the synchronized correct time must then be disseminated to all systems on an agency's network.

GUIDELINES

When evaluating the accuracy of a time source, agencies should consider the following:

- The location of the time source itself.
- The availability of the time source.
- The reliability of the time server to maintain accurate time received from the time source.
- The latency between the time source and agency systems.
- The reputation of the company hosting the time source.
- Configuring authentication mechanisms for clock synchronization with hosts.

ISO 17799: 2005 Reference

10.10.6 Clock synchronization

030213 Responding to System Faults

Purpose: To properly respond to faults and take corrective action.

STANDARD

All users and system administrators shall be responsible for reporting system faults (i.e., problems, errors and incidents) that affect routine operations to the appropriate authorized staff or third-party technician(s).

Staff shall describe the fault as clearly and completely as they can, and if a reason is known for the fault, the reason shall be provided as well.

Agency staff shall request that the authorized staff or third-party technician(s) log the fault, provide agency staff with a tracking or ticket number and implement clear procedures for handling the reported fault(s).

ISO 17799: 2005 Reference

10.10.5 Fault logging

030214 Managing or Using Transaction/Processing Reports

Purpose: To ensure that validation checks are incorporated to detect possible corruption or loss of system and data integrity.

STANDARD

For IT transaction records, which include access and audit logs related to the activities of IT systems, agencies must establish and maintain an adequate system of controls.

For financial transactions and accounting records the standard is addressed by the North Carolina Office of the State Controller.

ISO 17799: 2005 Reference

12.2.2 Control of internal processing

030215 Commissioning Facilities Management for Information Technology

Purpose: To ensure that information technology facilities are managed with regulatory security frameworks and provide effective planning and operation.

STANDARD

The agency's facilities management personnel shall work with appropriate departments (IT, Security, etc.) while fulfilling their duties to ensure that proper precautions are taken in regard to physical security, including:

- Limiting ingress and egress route vulnerabilities.
- Restricting available entrances, while emphasizing the availability of emergency exits.
- Assigning individuals to survey each area to ensure that all individuals have left the building.
- Building perimeter security considerations.

Agencies should establish the security of construction, modification, maintenance and related facility management concerns for facilities and premises within the care and custody of the agency or State.

If the agency determines to outsource its facilities management, the outsource vendor must comply with Standard 100103, Contracting with External Suppliers/Other Service Providers.

ISO 17799: 2005 Reference

6.2.1 Identification of risks related to external parties

030216 Third Party Service Delivery

Purpose: To define, monitor, and manage service levels from third party service providers.

STANDARD

When agencies contract with external service providers, service definitions, delivery levels and security requirements shall be documented in a formal service level agreement (SLA) or other documented agreement.

Agencies shall ensure that the SLA includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements.

Agencies shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Agencies shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.

Changes to the SLA and services provided shall be controlled through a formal change management process.

GUIDELINES

See ISO 17799, section 6.2.3, Addressing security in third party agreements, for the security-related topics that should be addressed in the SLA or third party agreement.

ISO 17799: 2005 References

10.2 Third party service delivery management

030217 Log-on Procedures

Purpose: To reduce the risk of unauthorized system access.

STANDARD

Agencies shall develop secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall be designed to minimize the risk of unauthorized access.

Agencies shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use.

Agencies shall configure systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the established limit, the configuration shall either force a time delay before further log-on attempts are allowed or shall disable the user account such that it can only be reactivated by a system administrator.

GUIDELINES

When developing the secure log-on procedures, agencies should include the following considerations.

- Do not display information about the system or services until the log-on process has successfully completed.
- Log on windows should display a minimal amount of information.
- Do not validate the log-on process until all log-on data is input. Failing the process as each input field is completed will provide an attacker with information to further the attack.
- Display only generic “log-on failed” messages if the user does not complete the log-on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect.

Also see Standard 020106, Managing Passwords, for instructions that complement this standard.

ISO 17799: 2005 Reference
11.5.1 Secure log-on procedures

030218 System Utilities

Purpose: To control the use of system utilities that can bypass or override security controls.

STANDARD

Access to system utilities that are run with elevated privileges capable of bypassing or overriding system or application controls shall be strictly limited to users and administrators with a recurring need to run or use those utilities. Other uses of and access to those utilities shall only be granted on a temporary basis.

These system utilities shall be segregated from other applications and software such that they can only be accessed by authorized users.

GUIDELINES

Agencies should develop procedures for granting and documenting authorization for specific individuals to use powerful system utilities, whether or not such use is temporary.

Use of system utilities should be audited or logged.

Agencies should remove or disable system utilities that are not needed.

Agencies should consider whether granting authorization for an individual to use a system utility may violate segregation of duties if the utility allows bypassing or overriding of segregation controls. If granting authorization to use a system utility could potentially violate segregation controls, the agency shall enact precautions to ensure that this violation does not occur. Detailed auditing or two-person control could provide assurance that segregation of duties is maintained.

ISO 17799: 2005 Reference
11.5.4 Use of system utilities

030219 System Use Procedures

Purpose: To detect unauthorized activity.

STANDARD

Agencies shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity.

All network components and computer systems used for agency operations must have the audit mechanism enabled and shall include logs to record specified audit events.

Audit logs, whether on-line or stored on backup media, shall be protected so that no users, including system administrators, can alter them.

GUIDELINES

For audit logs on internal agency systems and network components, agencies should record, at a minimum, the following types of security-related events:

- User login activity, both failed and successful, including user IDs, log-in date/time, log-out date/time.
- Unauthorized access attempts to network or system resources.
- Changes to critical application system files.
- Changes to system security parameters.
- System start-ups and shut-downs.
- Changes to the auditing function, including enabling or disabling auditing and changing events to be audited.
- User ID creation, deletion, and privilege change activity.
- All uses of special system privileges.

Agencies should ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations. Agencies should also ensure that on-line audit logs are backed-up to protected media well before the on-line logs are filled to capacity so that no audit information is lost or overwritten.

ISO 17799: 2005 Reference
10.10.2 Monitoring system use

030220 Internal Processing Controls

Purpose: To prevent corruption or loss of information in applications.

STANDARD

Agencies shall develop clear policies, standards, and/or procedures to detect, correct, and manage corrupted data files.

ISO 17799: 2005 Reference
12.2.2 Control of internal processing

030221 Corruption of Data

Purpose: To minimize and detect corruption or loss of information in applications.

STANDARD

The design of applications shall ensure that data validation controls are implemented to minimize the risk of processing failures leading to a loss of integrity and to detect any corruption of information through processing errors or deliberate acts.

GUIDELINES

Examples of controls that could be used to ensure data validation are:

- Add, modify, and delete functions should be carefully controlled.
- Automatic reconciling of balances from run-to-run or system-to-system can be implemented in systems to compare opening balances against previous closing balances.
- Processes should fail securely such that no further processing will occur. For example, internal controls in processes should be designed to detect if a process is running out of order or without the proper input and fail without further processing.
- Running hash totals of records or files can be maintained and compared to hash totals of backups or recovered records or files. They could also be compared run-to-run or system-to-system to ensure that the end of one transaction period is the same as the beginning of the next.

RELATED INFORMATION

030214 Managing or Using Transaction/Processing Reports

030220 Internal Processing Controls
030222 Corrupt Data Controls

ISO 17799: 2005 Reference
12.2.2 Control of internal processing

030222 Corrupt Data Controls

Purpose: To correct corrupted data and prevent corruption or loss of data in applications when recovering from system or processing failure.

STANDARD

The design of applications shall ensure that data validation controls are implemented such that agencies can correct corrupted data. These controls shall also ensure the correct processing of data in the event of recovery from system or processing failure.

GUIDELINES

An example of a method to rebuild corrupted records or files from a last known good state is a transaction log or log of activities. Agencies should take precautions to ensure that the transaction or activity log does not contain the action that corrupted the data in the first place.

RELATED INFORMATION

030214 Managing or Using Transaction/Processing Reports
030220 Internal Processing Controls
030221 Corruption of Data

ISO 17799: 2005 Reference
12.2.2 Control of internal processing

030223 Controlling On-Line Transactions

Purpose: To protect on-line transactions and the parties involved in on-line transactions.

STANDARD

When agencies accept or initiate on-line transactions, they shall implement controls or verify that controls exist to:

- Validate the identity of the parties involved in the transaction.
- Gain proper approval for the transaction, if necessary.
- Protect the confidential data involved in the transaction.
- Ensure the integrity of the transaction.
- Obtain proof that the transaction is completed correctly.
- Prevent unauthorized or accidental replay of a transaction so that it will not be duplicated.

GUIDELINES

Methods to implement the controls above are dependent on the nature of the transaction and the level of risk but could include:

- Using electronic signatures that are validated through an approved, known certificate authority (CA).
- Using enhanced authentication techniques, such as multi-factor authentication.
- Implementing automated two-person controls for approving transactions.
- Encrypting the message content when transmitted over an unsecured communications link.
- Encrypting the communications link through secure protocols.
- Storing transaction details in a secure location not accessible to unauthorized persons.

ISO 17799: 2005 Reference
10.9.2 On-Line Transactions

Section 03 E-mail and the Worldwide Web

030301 Downloading Files and Information from the Internet

Purpose: To establish restrictions pertaining to downloading files and use of the Internet.

STANDARD

Personnel shall only download files that aid in the performance of work-related functions. While downloading files or information from the Internet, State employees and State network users shall comply with the agency's acceptable use policy and the statewide standards that address desktop and laptop security, including those listed below.

Safeguards that shall be in place to limit the risk of downloading files that may contain malware include, but are not limited to:

- Use of antivirus software that scans files before they are downloaded
- Contacting a system administrator before directly adding any software to the system that is outside of the standard installation package
- Validating before installation the source of software and the reputation of the site from which it is downloaded
- Not opening files from people not known to the user or files that are spammed via email
- Not downloading free or heavily discounted software that is ordinarily expensive
- Not downloading free trial software that may constitute a copyright or licensing violation or implicate the State for licensing agreements
- Not downloading files via peer-to-peer (P2P) applications

020103 – Securing Unattended Work Stations

020106 – Managing Passwords

030902 – Loading Personal Screensavers

050402 – Issuing Laptop/Portable Computers to Personnel

050403 – Using Laptop/Portable Computers

050408 – Day to Day Use of Laptop/Portable Computers

050705 – Clear Screen

050706 – Logon and Logoff from your Computer

ISO 17799: 2005 References
10.4.1 Controls against malicious code
11.1.1 Access control policy

030302 Using and Receiving Digital Signatures

Purpose: To protect the integrity of State data through the use of digital signatures.

STANDARD

A public key infrastructure (PKI) for issuing and managing digital certificates and digital signatures to State employees is an enterprise-wide infrastructure. It must be implemented and maintained by ITS as a statewide initiative.

Digital certificates are a core technology for securing the State's infrastructure. Digital certificates provide strong and flexible authentication services for individuals and applications and must be consistent with the architecture and standards in the Statewide Technical Architecture. The enterprise PKI must meet the following requirements:

- Security — an enterprise PKI provides a secure environment for generation, distribution, and management of encryption keys and digital certificates. It supports strong authentication, minimizes application-based passwords and integrates into the State's security infrastructure.
- Management — a certificate authority[3] (CA) provides secure storage of master keys used to sign digital certificates for State employees. Digital certificates are stored in the State's enterprise directory tree. Registration authority[4] for issuing and revoking certificates is delegated to State agencies.
- Consistency — an enterprise PKI ensures that digital certificates will be issued and managed to minimize interoperability and acceptance problems. A lack of consistency will increase infrastructure management costs for security.
- Operation — an enterprise PKI, operated seven (7) days per week and twenty-four (24) hours per day, is required to ensure that proper security services are available. Unscheduled service interruptions interfere with conducting the State's electronic business securely as well as with worker productivity.
- Scalability — an enterprise PKI is required to support long-term needs for statewide security of networks, systems, and data. There shall be no technical limitation that precludes servicing any audience permitted by general statute.

[3] A CA maintains a highly secure environment to ensure that master keys and certificate generation cannot be compromised.
[4] A registration authority authorizes requests for digital certificates, verifies the identity of requestors and authorizes revocation of digital certificates.

ISO 17799: 2005 Reference
10.9.1 Electronic commerce

030303 Sending Electronic Mail

Purpose: To establish requirements for sending electronic mail.

STANDARD

Agencies shall develop policies regarding unacceptable use of email and set forth the extent to which users may use agency-provided email for personal use. Agencies that connect to the State Network are subject to the statewide acceptable use policies.

Examples of email content that constitute unacceptable use are:

- Private or personal for-profit activities. This includes personal use of email for marketing or business transactions, advertising of products or services or any other activity intended to foster personal gain.
- Unauthorized not-for-profit business activities.
- Use for, or in support of, unlawful/prohibited activities as defined by federal, State and local laws or regulations. Illegal activities relating to Internet and network access include, but are not limited to:
  - Tampering with computer hardware or software.
  - Knowingly vandalizing or destroying computer files.
  - Transmitting threatening, obscene or harassing materials.
  - Attempting to penetrate a remote site/computer without proper authorization.
  - Using the Internet in an effort to access data that are protected and not intended for public access.
  - Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret.
  - Intentionally seeking information about, obtaining copies of or modifying contents of files, other data or passwords belonging to other users, unless explicitly authorized to do so by those users.
- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
- Deliberate interference or disruption of another user's work or system. Users must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance) or the introduction of computer worms or viruses by any means.
- Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.
- Unauthorized distribution of State data and information.

ISO 17799: 2005 References
10.8.2 Exchange agreements
10.8.4 Electronic messaging
12.2.3 Message integrity

030304 Receiving Electronic Mail

Purpose: To provide security training for receiving electronic mail.

STANDARD

Agencies shall provide training on the security issues involved in receiving email that addresses unsolicited mail, attachments and malicious code.

Agencies shall also establish procedures that address the following issues:

- Attacks on electronic mail (e.g., viruses, interception, user identification, defensive systems).
- Protection of electronic mail attachments using such techniques as filtering, stripping and store and forward.
- Use of cryptography to protect the confidentiality and integrity of electronic messages.

ISO 17799: 2005 References
10.4.1 Controls against malicious code
12.2.3 Message integrity

030305 Retaining or Deleting Electronic Mail

Purpose: To provide guidance on retaining or deleting electronic mail (email).

STANDARD

Communications sent or received by agency email systems may be records as defined by the North Carolina Public Records Law, N.C.G.S. §§132.1, *et seq.,* and shall be managed according to the requirements of an agency's record retention policy or as set forth in the General Schedule for Electronic Records published by the Department of Cultural Resources.

ISO 17799: 2005 References
15.1.3 Protection of organizational records

030306 Setting Up Intranet Access

Purpose: To implement and manage an agency Intranet in a secure manner.

STANDARD

Agencies that have Intranet sites shall provide the same controls on access to the Intranet site as to the files located on the network, in accordance with Standard 020101, Managing Access Control, and Standard 020108, Restricting Access to Information Systems.

Traffic to the Intranet site from an external location shall be blocked unless it is tunneled through a virtual private network (VPN).

GUIDELINES

When setting up access to the Intranet, agencies should implement the following best practices:

- A documented approval process should be created before any information is posted to the Intranet site.
- Before posting material to the Intranet, workers should be required to thoroughly check all information and programs to make sure they do not include viruses, Trojan horses, or other malicious code.

- All legal issues such as disclosure of confidential information and copyright infringement should be resolved prior to posting.

ISO 17799: 2005 References
11.1.1 Access control policy

030307 Setting Up Extranet Access

Purpose: To establish requirements for third parties to connect to State and agency networks.

STANDARD

Agencies that have Extranet sites shall provide the same access controls to the Extranet site as to the files located on the internal network, in accordance with Standard 020101, Managing Access Control and Standard 020108, Restricting Access to Information Systems.

All new connections between third parties and State agencies shall be documented in an agreement that includes information technology security requirements for the connections. The agreement shall be signed by an agency employee who is legally authorized to sign on behalf of the agency and by a representative from the third party who is legally authorized to sign on behalf of the third party. The signed document must be kept on file with the relevant extranet/network group:

GUIDELINES

Before placing a new Extranet into production, agencies should conduct a risk and/or business impact analysis.

When setting up access to the Extranet, agencies should implement the following best practices:

- A documented approval process should be created before any information is posted to the Extranet site.
- Before posting material to the Extranet, workers should be required to thoroughly check all information and programs to make sure they do not include viruses, Trojan horses or other malicious code.
- Workers should also be required to confirm the information's accuracy, timeliness and relevance to the agency's mission before posting it.
- Likewise, all legal issues such as disclosure of confidential information and copyright infringement should be resolved prior to posting.

ISO 17799: 2005 References
11.1.1 Access control policy

030308 Setting Up Internet Access

Purpose: To protect information technology resources from malicious attack and/or misuse.

STANDARD

Persons responsible for setting up Internet access for an agency shall ensure that the agency's network is safeguarded from malicious external intrusion by deploying, at a minimum, a configured and managed firewall. The configuration shall ensure that only the

minimum services are installed to allow the business functions. All unnecessary ports and services shall be uninstalled or denied.

ISO 17799: 2005 References
11.1.1 Access control policy

030309 Developing a Web Site

Purpose: To provide protection of information technology resources when developing Web sites.

STANDARD

Agencies shall use only qualified personnel to develop Web sites. Web site development shall incorporate secure-development best practices. Development Web sites shall be isolated from production networks to prevent remote compromise while the server is being built and the Web application developed. Development servers/applications shall be developed and tested with input validation to protect against data validation weaknesses in the Web application's design.

GUIDELINES

Industry standards for securing operating systems and Web server software, such as National Security Agency (NSA) and SANS Institute guidelines, should be used for guidance in securely configuring and hardening Web sites.

A Web server operating system and its related applications should have the latest patches installed to protect against known patch-related vulnerabilities.

Network and application (Web/database) vulnerability scans should be run against development servers during and after the development process to ensure that a server/Web application is built securely.

Any passwords used by a server, Web server, Web application, or any other related applications need to meet complexity levels and have change cycles appropriate to the level of risk posed by potential compromise of the system.

Completed Web sites should be periodically searched with a Web search engine by development staff to ensure that there is no access to Web information beyond what is intended.

Because of the public nature of Web servers, the use of file-integrity-checking software to detect the modification of static or critical files on the server is strongly recommended.

Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments.

ISO 17799: 2005 References
10.9.1 Electronic commerce

030310 Receiving Misdirected Information by Email

Purpose: To establish rules for the handling of misdirected email.

STANDARD

Misdirected or unsolicited email shall be treated with caution and not opened or responded to.

Agencies shall develop policies and/or training to educate users about the potential security risks involved in responding to unsolicited commercial email (spam), including responding to an invitation contained in such email to have one's email address removed from the sender's list.

GUIDELINES

Agencies should follow best practices relating to email by:

- Installing spam-filtering software on the email server.
- Installing personal desktop firewalls on user computers to prevent the internal spreading of spam- or email-borne viruses.
- Configuring a packet-screening firewall to safeguard agency networks from unsolicited activity.
- Providing informational notices requesting that users not reply to spam.

ISO 17799: 2005 References
10.8.4 Electronic messaging

030311 Forwarding Email

Purpose: To establish rules for properly forwarding email.

STANDARD

Agencies shall develop policies to encourage due care by users when forwarding messages so that users do not:

- Knowingly send out an email message that contains viruses, Trojan horses or other malware.
- Use the electronic-mail system or network resources to propagate chain letters, misinformation or hoax information.
- Forward any confidential information to any unauthorized party without the prior approval of a local department manager.
- Forward the wrong attachment.
- Send information or files that can cause damage to the State of North Carolina or its citizens.
- Send large files (over one [1] megabyte) to individuals, as these files may have an undesired effect on the response and stability of the electronic-mail system.
- Send unsolicited messages to large groups of people except as required to conduct agency business.

GUIDELINES

Agencies should consider including these items in an agency's individual acceptable use policy.

ISO 17799: 2005 References
10.8.4 Electronic messaging

030312 Using the Internet for Work Purposes

Purpose: To provide rules for the State's infrastructure and Internet use.

STANDARD

While performing work-related functions or while using publicly owned/publicly provided information-processing resources, State employees and authorized users shall use network resources and the Internet responsibly. Users accessing the State Network shall use resources responsibly in such a manner as to:

- Ensure that there is no intentional use of such services in an illegal, malicious or obscene manner.
- Ensure compliance with State and agency acceptable use policies.
- Ensure that all applicable software copyright and licensing laws are followed.
- Guard against wasting State Network resources.
- In addition, users of the State Network shall:
  - Not use the State Network for distributing unsolicited commercial advertising or personal Web hosting.
  - Avoid using Internet streaming sites except as consistent with the mission of the agency and for the minimum amount of time necessary to obtain the desired amount of information.
  - Not take actions that would constitute a criminal offense or make the State liable to civil suits, such as stalking, or actions that are abusive, fraudulent, hateful, defamatory, obscene or pornographic in content.
  - Not access or attempt to gain access to any computer account or network that they are not authorized to access.
  - Not intercept, attempt to intercept, forge or attempt to forge data transmissions that they are not authorized to access or send.

GUIDELINES

Agencies should consider including these items in an agency's individual acceptable use policy.

ISO 17799: 2005 References
11.1.1 Access control policy

030313 Giving Information When Ordering Goods on the Internet

Purpose: To provide awareness that there are potential security risks in revealing confidential information when ordering items via the Internet.

STANDARD

State employees who are responsible for ordering goods and services via the Internet must be cognizant that they are responsible for protecting State information.

When making payments via the Internet, personnel must:

- Ensure that all State credit or debit card details are kept confidential (including personal identification numbers [PINs], account numbers and details).
- Make every effort to verify that the third party is a legitimate e-business.
- Consider potential risks involved in conducting business on a Web site that has been compromised or is insecure.
- Verify that the third party is using the desired secure Web site by checking that the site address starts with https, not http, and that the Web uniform resource locator (URL) is accurate and has been typed in directly.

- Revert to ordering goods via telephone if any doubts or suspicions arise.
- Reconcile any credit card(s) used against credit card statements and scan statements for fraudulent or bogus charges.

ISO 17799: 2005 References
10.9.1 Electronic commerce
10.9.3 Publicly available information

030314 Out-of-the-Box Web Browser Issues

Purpose: To ensure the proper settings of Web browsers and other Internet software.

STANDARD

Agencies shall ensure that Web browser software is properly configured to protect the State's information technology systems.

System administrators, support personnel, and system users must be aware that:

- Most Web servers automatically collect information about any user visiting the site, including the user's Internet Protocol (IP) address, browser type and referrer, by reading this information (which every browser provides) from the user's browser.
- They should never run any programs that they are prompted to download.
- Confidential data may be stored on cookies on their machine automatically and that these cookies are updated automatically.
- Viruses, spyware, Trojan applications and other malicious code may be able to cause damage to the State's infrastructure via Web browsers.
- They must use built-in security features to ensure the best security for Web browsers.
- Web browser vulnerabilities must be routinely addressed through the distribution of any software patches needed to mitigate the vulnerabilities.

GUIDELINES

Support personnel should consider removing cookies from machines on a regular basis and scanning for spyware that may reside on Web browsers.

ISO 17799: 2005 References
10.9.3 Publicly available information

030315 Using Internet Search Engines

Purpose: To encourage users to verify information gathered from the Internet

STANDARD

Users of Internet search engines shall take precautions to verify the integrity of the information provided by the search engine. As users collect information gathered from the Internet, they must:

- Check data for their integrity and accuracy before using them for business purposes.

- Observe all copyrights, end user licensing agreements, and other property rights.
- Use caution when downloading files from Web sites, ensuring that all downloads are scanned for viruses and other malicious code.

ISO 17799: 2005 References
10.9.1 Electronic commerce

030316 Maintaining your Web Site

Purpose: To protect and maintain the State's Web sites

STANDARD

Agencies shall designate qualified individuals to administer and maintain their Web sites.

Agency management and agency system administrators shall ensure that:

- Agency Web sites are kept up to date and secure and the information they present is accurate.
- Public Web sites are hardened and standard security configurations, based on industry guidelines and State standards, are adhered to.
- Secure authentication is used to protect the security of Web servers that have access to confidential information or that perform critical functions.
- Web sites have the latest operating system and application patches.
- Web site logs are periodically reviewed.
- The number of personnel with administrative access is limited to only qualified individuals.
- The sites are available to the appropriate users (public and private).
- Unauthorized modification of the Web site information is quickly discovered and resolved.
- All sites that an agency is responsible for are periodically tested for vulnerabilities.
- All sites comply with all applicable laws and regulations.

GUIDELINES

Agencies should review and update the data contained within their Web sites on a six-month basis.

ISO 17799: 2005 References
10.9.1 Electronic commerce

030317 Filtering Inappropriate Material from the Internet

Purpose: To protect the State from the accessing of inappropriate Internet sites and material.

STANDARD

If an agency determines that it should filter access to Internet sites and materials, it shall develop a policy that sets forth the criteria by which it will determine when filtering will be performed and shall notify users of the policy. The implementation of access controls or

other techniques to filter out inappropriate Internet sites and materials may be necessary to protect network resources and ensure that:

- Employees do not accidentally or deliberately view, access or download inappropriate materials from the Internet that may cause concern or distress to themselves or other employees.
- Employees are restricted from inappropriate use that may result in criminal or civil penalties to the agency or State.
- Corrective actions can be taken for repeated instances of inappropriate use.

GUIDELINES

Agencies should consider the installation of a proxy server, content filtering appliance or intrusion detection or prevention devices.

ISO 17799: 2005 References
11.1.1 Access control policy

030318 Certainty of File Origin

Purpose: To protect the State from incorrect, malicious or inappropriate data.

STANDARD

When possible, information or computer file originality and authenticity should be verified to ensure that:

- No malicious or unauthorized software is downloaded.
- Decisions that depend upon the information or computer file are made using data that are as accurate as possible.

ISO 17799: 2005 References
10.4.1 Controls against malicious code

030319 Electronic Business Communication

Purpose: To identify the risks of using electronic business communications.

STANDARD

Agencies shall perform a risk assessment to identify the specific risks of using electronic business communications such as e-mail, instant messaging, and electronic data interchange (EDI). The risk assessment results shall be used to identify the policies and controls that are required to appropriately protect these communications.

GUIDELINES

The risk assessment should include the following considerations:

- Communications sensitivity — what are the consequences of unauthorized or accidental access, modification, or loss of the communications? Is there a consequence for misdirected or incorrectly addressed messages?
- Denial of service and impact on business processes—are communications time sensitive? Is reliability and availability of the communications service a factor?

- Legal considerations — are there requirements for proof of origin, delivery, and/or acceptance? Is non-repudiation a factor such that the sender cannot claim that they did not send or receive a message?
- Remote user access — are controls needed to allow secure remote access to e-mail accounts?

ISO 17799: 2005 References
10.8.4 Electronic messaging

030320 Standard on Electronic Business Communications

Purpose: To prevent corruption or loss of information in applications.

STANDARD

Agencies shall develop clear policies, standards, and/or procedures to detect, correct, and manage corrupted data files.

ISO 17799: 2005 References
10.8.4 Electronic messaging

030321 Cryptographic Keys

Purpose: To minimize and detect corruption or loss of information in applications.

STANDARD

The design of applications shall ensure that data validation controls are implemented to minimize the risk of processing failures leading to a loss of integrity and to detect any corruption of information through processing errors or deliberate acts.

GUIDELINES

Examples of controls that could be used to ensure data validation are:

- Carefully controlled add, modify, and delete functions.
- Implementation of automatic reconciling of balances from run-to-run or system-to-system in systems to compare opening balances against previous closing balances.
- Requiring that processes fail securely such that no further processing will occur. For example, internal controls in processes should be designed to detect if a process is running out of order or without the proper input and fail without further processing.
- The maintenance of running hash totals of records or files and the comparison of those records and files to hash totals of backups or recovered records or files. They could also be compared run-to-run or system-to-system to ensure that the end of one transaction period is the same as the beginning of the next.

ISO 17799: 2005 References
12.3.2 Key management

030322 Key Management Procedures

Purpose: To correct corrupted data and prevent corruption or loss of data in applications when recovering from system or processing failure.

STANDARD

The design of applications shall ensure that data validation controls are implemented such that Agencies can correct corrupted data. These controls shall also ensure the correct processing of data in the event of recovery from system or processing failure.

GUIDELINES

An example of a method to rebuild corrupted records or files from a last known good state is a transaction log or log of activities. Agencies should take precautions to ensure that the transaction or activity log does not contain the action that corrupted the data in the first place.

ISO 17799: 2005 References
12.3.2 Key management

030323

Controlling Mobile Code

Purpose: To protect the State Network from mobile code that performs unauthorized and malicious actions.

STANDARD

Agencies should develop a policy to protect the State Network and local networks from mobile code that may perform unauthorized and harmful actions. Active X and Java are examples of mobile code that can inadvertently breach your network defenses.

GUIDELINES

Agency policy should be developed based on the level of access and the level of risk the agency is willing to accept. Listed below are sample access and security settings that an agency may use to refine their policy.

- **Internet Server Usage.** These policies would cover the usage of mobile code served via the Internet by the organization's servers. A typical security setting should be high.
- **Internet Client Usage.** These policies would cover which categories of mobile code a client or user could access via the Internet. A typical security setting should be medium.
- **Intranet Usage**. These policies would cover the usage of mobile code only on the organization's intranet. A typical security setting might be medium or medium low.
- **Mobile Device Usage.** Similar to an Internet client, these policies are for mobile devices accessing various mobile code resources. A typical security setting might be medium.

Security Settings

1. HIGH
    a. The safest way to browse but also the least functional
    b. Few secure features are disabled
    c. Appropriate setting for avoiding sites that may have harmful content

2. MEDIUM
    a. Safe browsing and still functional
    b. Prompts before downloading potentially unsafe content
    c. Unsigned ActiveX controls are not downloaded
    d. Appropriate setting for most Internet sites

3. MEDIUM-LOW
    a. Same as Medium without prompts
    b. Most content will be run without prompts
    c. Unsigned ActiveX controls will not be downloaded
    d. Appropriate for sites on your local network (Intranet)

4. LOW
    a. Minimal safeguards and warning prompts are provided
    b. Most content is downloadable and run without prompts
    c. All active content can run
    d. Appropriate for sites that you absolutely trust

ISO 17799: 2005 References
10.4.2 Controls against mobile code

Section 04 Telephones and Fax

030401 Making Conference Calls

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

Confidential information shall not be discussed on speakerphones or other electronic media, including Voice over IP systems, during conference calls unless:

- All authorized parties participating in the call have been authenticated.
- All authorized participating parties have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation.
- The conference call is made in an area of the building that is secure (i.e., offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls).
- All parties involved in the conference call are openly identified.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030402 Using Videoconferencing Facilities

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

Confidential information shall not be discussed on videoconferences or other electronic media, including Voice over IP, unless:

- All authorized participants have been authenticated.
- All authorized participants have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation.
- The videoconference call is being made in an area of the building that is secured (i.e., offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls).
- All parties involved in the conference call are openly identified.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030403 Recording of Telephone Conversations

Purpose: To establish requirements for policies that disclose to employees and third-party contractors using State telephone systems that their use of such systems may be monitored.

STANDARD

Agencies shall have the right and ability to monitor the use of government telephones by employees and third-party contractors, including the recording of telephone conversations conducted on government telephone equipment.

State agencies using monitoring technologies shall establish policies to provide appropriate notice to State employees and third-party contractors of what the agency will be monitoring. The policies shall include the circumstances under which the monitoring will take place.

GUIDELINES

- Specify the scope and manner of monitoring for telephones and never exceed the scope of any written monitoring statement in the absence of any clearly stated exception.
- When appropriate, obtain a written receipt from State employees and third-party contractors acknowledging that they have received, read and understood the agency's monitoring policy.
- Inform State employees and third-party contractors of any activities that are prohibited when using agency telephones.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030404 Receiving Misdirected Information by Facsimile

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

When an agency receives a facsimile in error (wrong number, person, office, location or department), it shall notify the sender, if appropriate.

Misdirected facsimiles shall be treated as confidential documents and shall be shredded.

Facsimiles that carry advertisements may be discarded.

RELATED INFORMATION

Standard 030408 – Receiving Unsolicited Facsimiles

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030405 Giving Information When Ordering Goods on Telephone

Purpose: To provide awareness that giving information over the telephone presents security risks

STANDARD

When confidential information (e.g., credit card number, social security number) is required while conducting business (i.e., ordering goods) using the telephone, employees must ensure that they know exactly to whom they are speaking and whether that person is authorized to receive such information:

- Confidential information must not be left on answering machines or other recording devices.
- Care must be taken to ensure that confidential information cannot be overheard when it is disclosed over the telephone.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030406 Persons Giving Instructions over the Telephone

Purpose: To ensure that confidential information is provided only to authorized individuals

STANDARD

To reduce the possibility that confidential information will be provided to unauthorized individuals, agencies shall establish procedures for employees and contractors to follow when conveying confidential information over the telephone, including verifying that the recipients of the information are who they say they are. Agencies shall also provide employees and contractors with awareness training on social engineering and the legal requirements for protecting confidential data.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures

030407 Persons Requesting Information over the Telephone

Purpose: To require that the identity of persons requesting confidential information over the phone is verified.

STANDARD

If confidential instructions or information are requested over the telephone, the identity of the caller shall be verified as a caller authorized to receive such information before the instructions or information is disclosed.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures
10.8.5 Business information systems

030408 Receiving Unsolicited Facsimiles

Purpose: To provide awareness of the responsibilities of parties receiving unsolicited or unexpected facsimiles

STANDARD

Agencies shall develop guidelines for handling the receipt of unsolicited facsimiles, including advertising material, as well as misdirected facsimiles.

RELATED INFORMATION
Standard 030404 – Receiving Misdirected Information by Facsimile

ISO 17799: 2005 References
10.8.5 Business information systems

Section 05 Data Management

030501 Transferring and Exchanging Data

Purpose: To protect the State's confidential information during the electronic exchange or transfer of data.

STANDARD

Agencies shall manage the electronic exchange or transfer of data to ensure that the confidentiality and integrity of the data are maintained during the transfer process. Agencies shall address the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the Internet, or exchange of electronic media and tapes.

ISO 17799: 2005 References
10.8.1 Information exchange policies and procedures

030502 Managing Data Storage

Purpose: To protect the State's information resident on electronic data storage

STANDARD

Agencies shall ensure the proper storage of data and information files for which they are responsible. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse. Agencies shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.

GUIDELINES

The primary security control available to agencies to protect confidential data in storage is using a State-approved data encryption method. Care should be taken to ensure that encryption keys are properly stored (separate from data) for later decryption.

RELATED INFORMATION

Chapter 9 - Dealing with Premises Related Considerations

ISO 17799: 2005 References
10.7.3 Information handling procedures
15.1.3 Protection of organizational records

030503 Managing Databases

Purpose: To protect the State's information databases.

STANDARD

Agencies shall properly safeguard the confidentiality (where applicable), integrity and availability of their databases. Data from these databases shall be protected from unauthorized deletion, modification or misuse and shall meet all applicable statutory and regulatory requirements.

GUIDELINES

To maintain the reliability of databases maintenance must be performed on the operating system of the system that hosts the databases, or there is a greater possibility that the database itself will fail.

Databases that store critical, confidential information such as client records, accounting data, medical history data and data on sales and purchases should require more stringent mean time between failures (MTBF) and mean time to repair (MTTR) configurations.

ISO 17799: 2005 References
12.2 Correct processing in applications
15.1.3 Protection of organizational records

030504 Permitting Emergency Data Amendment

Purpose: To protect the State's information

STANDARD

Agencies shall establish change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures.

All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.

ISO 17799: 2005 References
12.5.1 Change control procedures

030505 Receiving Information on Disks

Purpose: To protect the State's information systems.

STANDARD

All data or files received by an agency on a diskette, compact disc (CD) or any other electronic medium from an external source shall be downloaded to an agency system only if:

- The data or files come from a known, trusted source.
- The data or files first pass virus scan using State approved and current antivirus software.

This standard applies as well to files obtained as e-mail attachments and through any other file transfer mechanism.

ISO 17799: 2005 References
10.4.1 Controls against malicious code

030506 Setting Up a New Folder/Directory

Purpose: To provide directory-level protection for the State's information resources.

STANDARD

Agencies shall establish rules for creating and managing access to directory structures based on the most restrictive set of privileges needed for the performance of authorized tasks. New directory/folder structures shall be designed with the appropriate access controls to restrict access to authorized personnel only.

New folders/directories shall prohibit the modification or deletion of files and folders from personnel other than the data creator/owner or system administrators. New folders/directories designed for holding confidential information shall be password protected.

GUIDELINES

Agencies should consider limiting the ability of users to create new folders/directories on network or shared drives, which could cause security vulnerabilities or cause data to be difficult (or impossible) to locate.

ISO 17799: 2005 References
11.11.1 Access control policy

030507 Amending Directory Structures

Purpose: To protect the State's information systems at the directory level.

STANDARD

Agencies shall establish and manage access controls governing the modification or amendment of the directory structures on network or shared drives.

GUIDELINES

Modification of directory structures by anyone other than the creator/owner or system administrators should be prohibited.

Agencies should consider password-protecting directories.

ISO 17799: 2005 References
11.1.1 Access control policy

030508 Archiving Documents

Purpose: To protect the State's archived information resources

STANDARD

The standard recommended by ISO 17799 for this category is covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

ISO 17799: 2005 References
15.1.3 Protection of organizational records

030509 Information Retention Standard

Purpose: To protect the State's information and comply with record retention statutes.

STANDARD

The standard recommended by ISO 17799 for this category is covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

ISO 17799: 2005 References
15.1.3 Protection of organizational records

030510 Setting Up New Spreadsheets

Purpose: To protect the State's confidential information on spreadsheets.

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate

GUIDELINES

To mitigate security issues with spread sheets, agencies should consider:

- Validating the formulas in the spread sheet
- Implement read, write and deletion controls on access to control the spreadsheet's distribution.
- Maintaining retention and version control
- Saving the spreadsheet in a directory that is backed up regularly.

ISO 17799: 2005 References
10.1.2 Change management
10.3.2 System acceptance

030511 Setting Up New Databases

Purpose: To protect the State's confidential information on databases.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

GUIDELINES

To mitigate security issues with spreadsheets, agencies should:

- Validate the formulas in the spreadsheet
- Implement read, write and deletion controls on access to the spreadsheet
- Control the spreadsheet's distribution.
- Maintain retention and version control
- Save the spreadsheet in a directory that is backed up regularly.

To mitigate security issues with databases, agencies should:

- Fully test any database before making it operational
- Control access levels (read, write, modify) to the database
- Validate all data before they are entered into the database
- Maintain retention and version control
- Control database reports distribution

ISO 17799: 2005 References
10.1.2 Change management
10.3.2 System acceptance

030512 Linking Information between Documents and Files

Purpose: To protect the State's confidential and critical information

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

GUIDELINES

If a State employee creates a link between documents or files containing confidential information, the confidential data affected by the link should be properly labeled and appropriately controlled.

To mitigate security issues with linkages, agencies should:

- Consider that:
  - They may not have control of source document and information.
  - It may be possible for documents to be changed without agency knowledge.
  - Validation of completeness of linked information may be required,
  - Retention and version control may be difficult to maintain.
  - Integrity of linked files can be compromised.
- Check links on at least a semiannual basis for validity.

ISO 17799: 2005 Reference
10.7.4 Handling information procedures

030513 Updating Draft Reports

Purpose: To protect the State's information contained in draft reports.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate. The Department of Cultural Resources, Government Records Branch, has established guidelines for addressing draft documents.

ISO 17799: 2005 References
10.3.2 System acceptance
11.1.1 Access control policy

030514 Deleting Draft Reports

Purpose: To protect the State's information contained on draft reports.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate. The Department of Cultural Resources, Government Records Branch, has established guidelines for addressing drafts.

ISO 17799: 2005 References
7.2.2 Information labeling and handling
11.1.1 Information handling policy

030515 Using Version Control Systems

Purpose: To protect the State's information via version control

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

ISO 17799: 2005 References
10.1.2 Change management

030516 Sharing Data on Project Management Systems

Purpose: To protect the State's confidential information while utilizing project management software.

STANDARD

Project management software that allows sharing of files and data containing confidential information shall be used to share data only if the appropriate security controls are properly configured and implemented.

Appropriate security controls shall include:

- Authentication controls to ensure that authorized users are identified.
- Access controls to limit an individual's access to only the confidential information necessary for that person to perform his/her project role.
- Authorization controls to enforce version control and record retention requirements such that only designated individuals are able to modify or delete sensitive or critical records.
- Audit controls that record individual actions on files and records.

These controls may be supplemented by operating-system-level controls (e.g., file and directory access control lists and system audit logs) only if the project management software does not bypass these controls.

ISO 17799: 2005 References
11.1.1 Access control policy

030517 Updating Citizen and Business Information

Purpose: To protect the confidentiality and integrity of the State's electronic information on citizens and businesses.

STANDARD

Only authorized individuals shall perform updates to citizen and business databases. When changing information, State employees must be diligent in protecting confidential information and shall adhere to all applicable laws and regulations. Access to customer confidential data shall be controlled through various access control mechanisms.

GUIDELINES

Agencies should provide the appropriate management structure and control to foster compliance with data protection legislation. Agencies may need to write the responsibility for data protection into one or more job descriptions to reach compliance.

ISO 17799: 2005 References
15.1.4 Data protection and privacy of personal information

030518 Using Meaningful File Names

Purpose: To improve the State's information handling through meaningful file-naming conventions.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

ISO 17799: 2005 References
7.2.2 Information labeling and handling

030519 Using Headers and Footers

Purpose: To protect the State's confidential information by utilizing headers and footers.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

GUIDELINES

State employees may consider using headers and footers to notify readers of files classified as confidential.

ISO 17799: 2005 References
7.2.1 Classification guidelines
7.2.2 Information labeling and handling

030520 Using and Deleting "Temp" Files

Purpose: To protect the State's confidential information residual on systems.

STANDARD

State employees must remove old or unnecessary "temp" files from their desktop and laptop to prevent unauthorized access of confidential information.

GUIDELINES

Some of the "temp" files that should be examined and removed are:

- Clipboard files.
- Printer files.
- Automatic saves.
- Temporary backups of "deleted files."
- Cached Web pages/uniform resource locators (URLs).
- Trash Can or Recycle Bin (should be emptied periodically).

ISO 17799: 2005 References
10.5.1 Information back-up

030521 Using Customer and Other Third-Party Data Files

Purpose: To protect the confidentiality and integrity of the State's customer and third-party information.

STANDARD

Agencies shall ensure that all confidential customer information and related files under the agency's control in electronic format are handled properly and secured accordingly. Use of customer and third-party files shall be in compliance with all relevant laws, regulations, statutes and intellectual property rights.

ISO 17799: 2005 References
15.1 Compliance with legal requirements

030522 Saving Data/Information by Individual Users

Purpose: To protect information utilized by individuals on their respective systems.

STANDARD

State employees shall periodically save data files from their desktop and laptop computers to an appropriate backup drive or disk.

GUIDELINES

Saving data to an appropriate backup drive will:

- Prevent loss of work product due to workstation malfunction.
- Facilitate backup/restoration of data and files.
- Facilitate maintenance of software/hardware on workstation.

ISO 17799: 2005 References
7.2.2 Information labeling and handling

Section 06 Backup, Recovery and Archiving

030601 Restarting or Recovering of Systems

Purpose: To ensure that agency information technology systems restart successfully after a voluntary or forced shutdown.

STANDARD

Agencies shall establish procedures for the adequate backup and the restarting or recovery of their information technology systems.

Procedures for the restarting of information technology systems shall be properly tested and documented.

These procedures shall:

- Document backup frequencies and schedules.

- Document where the correct system information backup medium is stored.
- Specify the approved processes for restoring the system.
- Be in compliance with agency change management procedures.
- Be tested on a regular basis, as established by agency management.
- Provide guidance for restart documentation.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Planning Project
Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105	Training and Staff Awareness on the Business Continuity Plan
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 17799: 2005 References
10.5.1 Information back-up

030602 Backing Up Data on Portable Computers

Purpose: To protect the State's information stored on mobile/portable computers via regular backup plans.

STANDARD

Agencies shall ensure that information stored on mobile/portable computing devices is regularly and properly backed up. Information stored on any mobile/portable computing device shall be backed up according to the schedule specified in the agencies' business continuity plans.

When a mobile/portable computer is outside a secure area, the backup medium must be kept separate from the mobile/portable computer.

Backup media shall be properly stored in a secure, environmentally controlled location with access control.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Planning Project
Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105	Training and Staff Awareness on the Business Continuity Plan
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 17799: 2005 References
11.7.1 Mobile computing and communications

030603 Managing Backup and Recovery Procedures

Purpose: To ensure recoverability and availability of the State's information technology resources.

STANDARD

Agencies shall manage the backup and recovery procedures of their information technology systems according to their business continuity plans. These plans must be properly documented, implemented and tested to ensure operational viability and their adherence to N.C.G.S. §147-33.89.

GUIDELINES

In managing backup and recovery procedures, agencies should consider establishing requirements that:

- Backup schedules meet business system requirements.
- Backup and restoration processes are tested on a regular basis.
- Backup facilities are adequate for minimum levels of operation.
- Retention periods of various data are based on operations, laws and regulations.
- Backup and recovery procedures are periodically reviewed and updated, as necessary.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Planning Project
Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105	Training and Staff Awareness on the Business Continuity Plan
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 17799: 2005 Reference
10.5.1 Information back-up

030604 Archiving Information

Purpose: To ensure that the State's archived data are appropriately preserved

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate. The Department of Cultural Resources, Government Records Branch, has established requirements for archiving records.

.

ISO 17799: 2005 References
10.5.1 Information back-up

030605 Archiving Electronic Files

Purpose: To protect the State's information through the archiving of relevant data.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate. The Department of Cultural Resources, Government Records Branch, has established requirements for archiving records.

GUIDELINES

Agencies should consult with the North Carolina Department of Cultural Resources, Government Records Branch, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived.

When archiving data associated with legacy systems, agencies should plan to provide a method of accessing those data.

ISO 17799: 2005 References
10.5.1 Information back-up

030606 Recovery and Restoring of Data Files

Purpose: To ensure the integrity of the State's information during recovery and restoration.

STANDARD

Agencies shall ensure the proper recovery and restoration of data files from their information technology systems according to their business continuity plans. These business continuity plans, procedures and media must be properly documented, implemented, stored and tested to ensure operational viability, reliable retrieval and adherence to N.C.G.S. §147-33.89.

Data recovery must be conducted by authorized parties and recovered data must be tested for potential corruption.

When recovering data, a test set of the data is selected as the data exist at a specific point in time. The recovered data are then compared to the test set and reviewed for their integrity.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Planning Project
Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105	Training and Staff Awareness on the Business Continuity Plan
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 17799: 2005 References
10.5.1 Information back-up
10.7.3 Information handling procedures

Section 07 Document Handling

030701 Managing Hard-Copy Printouts

STANDARD

The standard recommended for this section by ISO 177999 is not appropriate for a statewide information security standard. If appropriate, the standard should be addressed by agency senior management.

GUIDELINES

Agencies may want to consider establishing policies and procedures that ensure proper management and control of hard copy print outs that contain confidential information. Documents that contain confidential information should be restricted to authorized personnel. Any person who prints confidential data should label and control the original document in accordance with all applicable policies, statutes and regulation. Proper retention, archive and disposal procedures for such documents should be observed.

030702 Photocopying Confidential Information

Purpose: To protect the State's confidential hard-copy information

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

GUIDELINES

Agencies may want to consider establishing policies and procedures that ensure proper management and control of all photocopied documents that contain confidential information. Documents that contain confidential information should be restricted to authorized personnel. Any person who photocopies confidential information should label and control the original and copied documents, in accordance with all applicable policies, statutes, and regulations. Proper retention, archive, and disposal procedures for photocopied documents should be observed.

RELATED INFORMATION

Standard 010102	Setting Classification Standards—Labeling Information
Standard 030508	Archiving Documents
Standard 030509	Information Retention Standard

ISO 17799: 2005 References
10.7.3 Information handling procedures

030703 Filing of Documents and Information

Purpose: To protect the State's hard-copy document files.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

RELATED INFORMATION

Standard 010102	Setting Classification Standards—Labeling Information
Standard 030508	Archiving Documents
Standard 030509	Information Retention

ISO 17799: 2005 References
10.7.3 Information handling procedures

030704 The Countersigning of Documents

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
10.7.3 Information handling procedures

030705 Checking Document Correctness

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
10.7.3 Information handling procedures

030706 Approving Documents

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
10.7.3 Information handling procedures

030707 Verifying Signatures

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
10.7.3 Information handling procedures

030708 Receiving Unsolicited Mail

Purpose: To protect State resources.

STANDARD

Agencies shall protect State resources by not taking action on unsolicited commercial electronic mail.

RELATED INFORMATION

Standard 030304	Receiving Electronic Mail (Email)
Standard 030310	Receiving Misdirected Information by Email

ISO 17799: 2005 References
10.7.3 Information handling procedures

030709 Style and Presentation of Reports

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
10.7.3 Information handling procedures

030710 Transporting Confidential Documents

Purpose: To protect the State's confidential information during transport.

STANDARD

Agencies shall ensure that confidential information in electronic form is properly protected in transport or transmission.

RELATED INFORMATION

Standard 030801	Using Encryption Techniques
Standard 030803	Sending Information to Third Parties

ISO 17799: 2005 References
7.2.2 Information labeling and handling
10.8.3 Physical media in transit

030711 Shredding of Unwanted Hard Copy

Purpose: To protect the State's confidential information.

STANDARD

Agencies should follow the requirements of the Department of Cultural Resources as set forth in 7 NCAC 04M .0510.

RELATED INFORMATION

Standard 030508	Archiving Documents
Standard 030509	Information Retention

ISO 17799: 2005 References
10.7.2 Disposal of media

030712 Using Good Document Management Practices

Purpose: To protect the State's confidential information.

STANDARD

The standard recommended by ISO 17799 for this category is covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

GUIDELINES

Agencies should consider implementing practices and procedures that will ensure that electronic documents are properly managed throughout their life cycles. A combination of manual and technical processes may be used to implement document management.

RELATED INFORMATION

Standard 030501	Transferring and Exchanging Data
Standard 030502	Managing Data Storage
Standard 030503	Managing Databases
Standard 030504	Permitting Emergency Data Amendment
Standard 030505	Receiving Information on Disks
Standard 030506	Setting Up a New Folder/Directory
Standard 030507	Amending Directory Structures
Standard 030508	Archiving Documents
Standard 030509	Information Retention Standard
Standard 030510	Setting Up New Spreadsheets

Standard 030511	Setting Up New Databases
Standard 030512	Linking Information between Documents and Files
Standard 030513	Updating Draft Reports
Standard 030514	Deleting Draft Reports
Standard 030515	Using Version Control Systems
Standard 030516	Sharing Data on Project Management Systems
Standard 030517	Updating Customer Information
Standard 030518	Using Meaningful File Names
Standard 030519	Using Headers and Footers
Standard 030520	Using and Deleting “Temp” Files
Standard 030521	Using Customer and Other Third-Party Data Files
Standard 030522	Saving of Data/Information by Individual Users

ISO 17799: 2005 References
10.7.3 Information handling procedures

Section 08 Securing Data

030801 Using Encryption Techniques

Purpose: To protect the State’s confidential information using encryption techniques.

STANDARD

Each agency shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a third party not served by the State Network. Encryption techniques shall be employed when encryption is appropriate.

Agencies must ensure that only authorized personnel have access to the encryption keys to confidential information.

Agencies must provide for an encryption key escrow when necessary to provide future access to encrypted data.

Proper management control of encryption keys and processes must be ensured when archiving confidential electronic files or documents.

GUIDELINES

Agencies should consider encrypting all confidential information or data that would have an adverse impact on the agency’s services or functions if their confidentiality were compromised, especially when such information is transmitted to a third party not served by the State Network.

Agencies should use an encryption algorithm of, at a minimum, 128-bit strength or one of those accepted and approved by the National Institute of Standards and Technology.

RELATED INFORMATION

Standard 010101	Setting Classification Standards—Defining Information
Standard 010102	Setting Classification Standards—Labeling Information
Standard 010103	Setting Classification Standards—Storing and Handling Information
Standard 010104	Setting Classification Standards—Isolating Top Secret Information
Standard 010105	Setting Classification Standards—Classifying Information
Standard 010106	Setting Classification Standards—Custodians of Confidential Information
Standard 010107	Setting Classification Standards—Managing Network Security
Standard 030203	Controlling Data Distribution
Standard 030205	Managing Electronic Keys
Standard 030605	Archiving Electronic Files

ISO 17799: 2005 References
12.3.2 Key management
15.1.6 Regulation of cryptographic controls

030802 Sharing Information

Purpose: To protect confidential data belonging to North Carolina citizens.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

GUIDELINES

Agencies should consider training personnel on their duty to protect confidential information from unauthorized disclosure or modification, including training on applicable policies, statutes and records that apply when such information is released to a third party or shared with other agencies.

ISO 17799: 2005 References
7.2.1 Classification guidelines
15.1.4 Data protection and privacy or personal information

030803 Sending Information to Third Parties

Purpose: To protect the State's confidential information in dealings with third parties.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate

GUIDELINES

Agencies should consider protecting confidential information sent to third parties by developing processes, procedures and business agreements that set forth the allowable use and distribution of confidential information. Agreements for the exchange of information with third parties should clearly document the third party's commitment to ensuring the privacy of the State's information and the third party's obligations in regard to handling, storage and further dissemination, as well as the consequences of failing to fulfill these obligations

ISO 17799: 2005 References
10.8.3 Exchange agreements

030804 Maintaining Customer Information Confidentiality

Purpose: To protect the confidential information of individuals.

STANDARD

Agencies shall manage and protect electronic information received from customers, constituents and third parties in accordance with all applicable federal and State statutes and regulations.

Appropriate security controls shall be put in place to ensure the confidentiality, integrity, and availability of confidential customer, constituent, third-party or State information.

ISO 17799: 2005 References
15.1.4 Data protection and privacy of personal information

030805 Handling of Customer Credit Card Details

The standard recommended by ISO 17799 in this category is governed by policies and standards established by the Office of the State Controller

030806 Fire Risks to the State's Information

Purpose: To reduce the fire risks to the State's information.

STANDARD

Agencies shall take proper care to manage the risks of fire to the State's data and information technology resources.

Risk assessments shall be performed at all sites where agency information is processed or stored to determine the effectiveness of current controls and the facility's risk from fire and other environmental threats.

GUIDELINES

- Agencies should consider storing duplicate copies of information at alternate locations.
- Most file cabinets are not fire-, smoke- or water-safe.
- Agencies should consider a dry pipe sprinkler system to protect documents from destruction in cases in which the building's sprinkler system is triggered.

ISO 17799: 2005 References
9.2.2 Supporting utilities

030807 Sending Out Reports

Purpose: To ensure that data or software is appropriately secured when sent to third parties.

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate

GUIDELINES

When exchanging electronic data or software with third parties, agencies should consider all ensure that the data are correct, that the exchange is properly approved and that the third party has in place adequate security to protect the confidentiality (if applicable), integrity and availability of the data/software exchanged.

ISO 17799: 2005 References
10.8.2 Exchange agreements

030808 Dealing with Sensitive Financial Information

Purpose: To ensure strong control of financial information.

STANDARD

Agencies that have confidential financial information in electronic format shall deploy, test, assess and maintain adequate technical and administrative security controls to ensure the confidentiality, integrity and availability of the financial information.

GUIDELINES

Agencies should consider using separation-of-duties techniques for input and control of financial data.

To help ensure the confidentiality and (where applicable) the integrity of data at rest, it is recommended that agencies apply cryptographic algorithms of at least 128-bit strength to digital financial information.

RELATED INFORMATION

Standard 030901	Using Dual-Input Controls
Standard 030907	Need for Dual Control/Segregation of Duties

ISO 17799: 2005 References
7.2.1 Classification guidelines

030809 Deleting Data Created/Owned by Others

Purpose: To protect the integrity and availability of State data.

STANDARD

The standard recommended by ISO 17799 for this category is covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

GUIDELINES

Agencies should consider document handling procedures to properly manage the data for which they are responsible and guard against misuse or unauthorized deletions.

Agencies should consider employing mitigation techniques such as, but not limited to, the following:

- Password-protecting files and folders so that personnel other than the data custodian may not delete data that they are not responsible for.
- Version control methods for tracking of changes, so users will know if data have been altered and by whom.
- Daily, weekly and monthly backups for immediate recovery of deleted or changed data.

RELATED INFORMATION

Standard 030605 Archiving Electronic Files

ISO 17799: 2005 References
11.1.1 Access control policy

030810 Protecting Documents with Passwords

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate

GUIDELINES

Agencies should consider protecting confidential files with unique passwords to augment their current technical and administrative security access controls.

If agencies require passwords for confidential files, agencies should provide for a password escrow to facilitate future access to password-protected documents. File passwords should be used to augment access control mechanisms. They are not meant to replace strong access controls.

RELATED INFORMATION

Standard 020106 Managing Passwords

Standard 020108 Restricting Access to Information Systems

Standard 020110 Giving Access to Files and Documents

ISO 17799: 2005 References
11.1.1 Access control policy

030811 Printing Classified Documents

Purpose: To protect printed confidential documents.

STANDARD

Where possible, agencies shall develop and employ a process to properly clear the memory from a printer (or copier) that has been used to print confidential information. Authorized personnel must be present to safeguard the confidentiality of the material both during and after printing.

RELATED INFORMATION

Standard 010102 Setting Classification Standards—Labeling Information

Standard 010103 Setting Classification Standards—Storing and Handling Information

Standard 010104 Setting Classification Standards—Isolating Top Secret Information

Standard 010105 Setting Classification Standards—Classifying Information

Standard 010106 Setting Classification Standards—Custodians of Confidential Information

Standard 050205 Using Centralized, Networked or Stand-Alone Printers

Standard 030701 Managing Hard-Copy Printouts

ISO 17799: 2005 References
11.3.3 Clear desk and clear screen policy

Section 09 Other Information Handling and Processing

030901 Using Dual-Input Controls

Purpose: To protect information using dual-input comparisons.

STANDARD

Dual-input controls shall be used when data entry is critical to the business process. Agencies shall manage the input of financial information with the use of dual controls whenever possible.

ISO 17799: 2005 References
10.1.3 Segregation of duties

030902 Loading Personal Screen Savers

Purpose: To protect the State's assets by eliminating non-approved screen savers.

STANDARD

Personnel shall load only those screen savers that have been approved by their agencies.

Agencies shall train their employees on the risks of acquiring malware such as viruses, spyware and Trojan horses by downloading and installing unauthorized screen savers.

GUIDELINES

Personal screen savers can be resource intensive to computer systems. Agencies should strongly discourage downloading screen saver software from the Internet.

ISO 17799: 2005 References
10.4.1 Controls against malicious code

030903 Using External Disposal Firms

Purpose: To protect the State's assets during third-party disposal.

STANDARD

Agencies must ensure that all State/agency information is fully removed from obsolete information technology equipment and not recoverable before the equipment is released to the State Office of Surplus Property or a third-party disposal facility.

Agencies involved in the disposal of obsolete material shall utilize only companies that specialize in secure waste disposal and that can comply with service level agreements established by the agency. Service level agreements with external firms/third parties shall include, but not necessarily be limited to, the following:

- Stipulations to ensure compliance with the agency's security policies and standards, enforceable by suit for breach of contract.
- Development of procedure(s) for certifying that data have been properly removed from government-controlled equipment before it is transferred, resold, donated, or disposed of.
- Removal of data from floppy disks, CD-ROMs, magnetic tapes and all other electronic storage media or subsequent destruction (e.g., degaussing, shredding, etc).
- Scheduled disposal periods and/or processes involved in waste collection.

RELATED INFORMATION

Standard 050701	Disposing of Obsolete Equipment
Standard	State CIO Standards for Clearing or Destroying Media[5]

ISO 17799: 2005 References
6.2.3 Addressing Security in third party agreements
10.7.2 Disposal of media

030904 Using Photocopiers for Personal Use

STANDARD

The standard recommended by ISO 17799 for this category raises an issue for individual agencies to address, if appropriate.

ISO 17799: 2005 References
15.1.5 Prevention of misuse of information processing facilities

[5] See, State CIO Standard under "Other Security Policies and Standards"

030905 Speaking to the Media

STANDARD

The standard recommended by ISO 17799 in this section is not appropriate as an information technology security standard for North Carolina executive branch agencies.

030906 Speaking to Customers

STANDARD

The standard recommended by ISO 17799 in this section is not appropriate as an information technology security standard for North Carolina executive branch agencies.

030907 Need for Dual Control/Segregation of Duties

STANDARD

The standard recommended by ISO 17799 in this section is governed by individual agency requirements.

030908 Using Clear Desk Standard

Purpose: To reduce the risk of confidential information being viewed by unauthorized persons.

STANDARD

Agencies shall inform personnel of the risks involved in leaving confidential work on their computer screens while away from their desks.

Personnel shall be given training on this standard on an annual basis. The training shall include information on any civil or criminal penalties that may apply to individuals who breach confidentiality statutes.

GUIDELINES

Security measures that should be implemented include, but are not limited to:

- Shutdown/powering off of computers.
- Logging off or locking computers while away from the desk.
- Clearing all printers and fax machines of confidential printouts.

ISO 17799: 2005 References
11.3.3 Clear desk and clear screen policy

030909 Misaddressing Communications to Third Parties

Purpose: To reduce the risk of communicating misinformation or confidential information to unauthorized persons.

STANDARD

Agency personnel shall exercise due care when addressing email correspondence to ensure that the correspondence is addressed correctly and that the intended recipient is authorized to view content within emails or documents.

GUIDELINES

Agencies should encourage the attachment of a statement to email(s) that the message and any response to the message received by the agency are being sent on a State email system and may be subject to monitoring and disclosure to third parties, including law enforcement personnel.

An example is:

> Email correspondence to and from this sender may be subject to the North Carolina Public Records Law and may be disclosed to third parties, including law enforcement personnel.

Instructions and disclaimers shall be reviewed and approved by the agency or State legal staff prior to use.

RELATED INFORMATION

State CIO Policy and Procedures on Confidential Information Technology Security Records

ISO 17799: 2005 References
10.8.5 Business information systems

030910 Verifying Correctness of Information

Purpose: To reduce the risk of propagating incorrect information.

STANDARD

Agencies shall validate data output from application systems to ensure that the data-processing function correctly stores the data.

ISO 17799: 2005 References
12.2.4 Output data validation

030911 Traveling on Business

Purpose: To reduce the risk of losing State assets.

STANDARD

Agencies shall address employee responsibilities for safeguarding information technology assets and information when traveling on agency/State business. Agencies shall train their employees in regard to their responsibilities and provide guidance on how they can reduce the risks of disclosing confidential information and avoid having agency/State property stolen.

RELATED INFORMATION

Desktop and Laptop Security Standard

ISO 17799: 2005 References
11.7.1 Mobile computing and communications

030912 Checking Customer Credit Limits

The standard recommended by ISO 17799 in this section is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
15.1.4 Data protection and privacy of personal information

HISTORY (HISTORY TITLE)

State CIO Approval Date
Original Issue Date:
Subsequent History:

Policy Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Use of the State Network	030303 – Sending Electronic Mail 020121 – Acceptable Usage of Information Assets 100301 – Using the Internet in an Acceptable Way 030312 – Using the Internet for Work Purposes
Public Key Infrastructure and Digital Certificates	030302 – Using and Receiving Digital Signatures
Network Security Policy	030103 – Network Security
Remote Access Policy, including Mobile Computing and Telecommuting	020112 – Controlling Remote User Access 030103 – Accessing your Network Remotely 050404 – Working from Home or Other Off-Site Location (Teleworking)
Permanent Removal of Data from Electronic Media Standard	030903 –Using External Disposal Firms 040301 – Disposing of Software 050701 – Disposing of Obsolete Equipment
Desktop and Laptop Security Standard	020103 – Securing Unattended Work Stations 020106 – Managing Passwords 030902 – Loading Personal Screensavers 050402 – Issuing Laptop/Portable Computers 050705 – Clear Screen 050706 – Logon and Logoff from Your Computer
Remote Access Security Standard	020112 – Controlling Remote User Access 030103 – Accessing Your network Remotely